COMPARING STRASBOURG AND LUXEMBOURG CASE-LAW ON BULK INTERCEPTION OF PERSONAL DATA AND THEIR USE

Johan Callewaert

Brussels, Data Protection Day, 25 January 2024[1]

SPEAKING NOTES

Relevant case-law:

- ECtHR: *Big Brother Watch and Others v. the United Kingdom* and *Centrum för rättvisa v. Sweden*
- CJEU: *SpaceNet and Telekom Deutschland*

Main relevant European provisions:

- EU law:
  - Directive 2002/58 on the processing of personal data and the protection of privacy
  - Articles 7 and 8 of the EU-Charter
- Convention: Article 8

First finding: broad agreement between the two systems on the general objectives and principles:

- The need for the protection of citizens against abuse and arbitrariness in the collection and processing of their personal data
- The need for strong safeguards to prevent these risks from materialising

But different approaches as regards their implementation.

EU law approach

More rigid, but providing higher level of foreseeability:

- operating with pre-determined concepts, categories and safeguards,
- exhaustively listed
- triggering automatic consequences (leaving no discretion):
  - three categories of objectives: the protection of national security, public security and the protection against serious crimes
  - three categories of personal data: traffic and location data, IP addresses, mere civil identity of users
  - to be applied mechanically, i.e. the limits of what is allowed in terms of bulk interception will result automatically from the category of the data concerned and the category of purposes concerned
  - the same applies to the safeguards:
    - exhaustive list
    - resulting automatically from the pre-determined categories concerned
- highly protective test: strict necessity

[1] Panel 1: "A Tale of Two Courts: Lessons in Data Protection from Strasbourg and Luxembourg"

Convention approach

More flexible, more dynamic, but also more casuistic → reduced foreseeability

- No exhaustive list of pre-determined categories of risks or data
    - the scope for protection is open-ended
    - however, requirement that the grounds upon which bulk interception might be authorised be set out with sufficient clarity and detail
- No exhaustive list of pre-determined categories of data
    - the criterion is the interference with privacy rights, which can take on different forms
- Safeguards:
    - Longer list, containing some safeguards not required under EU law:
        - Need to set out the circumstances in which bulk interception is allowed
        - Need for an independent authorisation at the outset (decisive in BBW; CJEU ambiguous about this)
        - High degree of precision in the description of the grounds justifying interception
        - Identification of the selectors (decisive in BBW)
        - Procedures for the selection, examination and use of intercept material
        - Safeguards concerning the storage of the material
    - Not exhaustive: what matters is whether the safeguards are adapted and effective in the circumstances → the mix of safeguards can vary
    - "End to end"-safeguards: assessment at each stage of the process
    - Global assessment → some safeguards can compensate for the weakness of others
- Test: "narrower margin of appreciation"

Result: mixed picture:

- There is only partial convergence between the two regimes
- They can however be made compatible with each other
    - Importance: because national judges must apply EU law in compliance with the Convention

Guidance offered by both EU law and the Convention for dealing with duality of protection standards: Articles 52(3) of the EU-Charter and 53 of the Convention:

- 2 rules:
    1) The Convention protection standard is a minimum, applicable also under EU law
    2) This standard can be raised by EU law
- Consequently, national judges:
    1) Must go for the higher standard
    2) → Must compare the respective protection levels, in respect of each safeguard, i.e. take the best of the two worlds and combine them

Implementation: pragmatic approach, two steps:

- First step: Convention as starting point, for three reasons:
    - It is the mandatory minimum protection level, applicable also under EU law
    - It has the broader scope and the longer list of safeguards → higher chance of covering all the facts of the case

    - In order to be on the safe side: if the case comes to Strasbourg, only the compliance with the Convention will be tested

- Second step: raise the Convention standard wherever EU law so requires, e.g. as regards:
    - National security (in the strict sense) as the only ground allowing bulk interception of traffic and location data
    - The strict necessity test